Paragraphs 18-21
of
English translation

OIPE IAP79 APR 23 2007 PATENT & TRADEMARK OFFICE

with a network (Internet) through a serial port 15 and a modem, or a communication adapter 18 (Ethernet and token ring card), and this system 100 can perform a communication link with the computer of others [**** / transmitting a cryptographic key] etc. Moreover, a remote transmitter-receiver machine can be connected to a serial port 15 or a parallel port 16, and data can be transmitted to it and received by infrared radiation or the electric wave (for example, transmission of the cryptographic key to an addressee etc.).

[0015] By the audio controller 21, a loudspeaker 23 receives the sound signal by which D/A (digital to analog) conversion was carried out through amplifier 22, and outputs it as voice. Moreover, the audio controller 21 carries out A/D (analog to digital) conversion of the speech information received from the microphone 24, and makes it possible to be crowded for a system in the speech information of the system exterior.

[0016] Thus, the cryptographic key generative system and cryptographic key distribution system of this invention could understand easily that it can carry out with the communication terminals containing various home electronics, such as television having the usual personal computer (PC), a workstation, Notebook PC, a palm top PC and a network computer, and a computer, the game machine which has communication facility, a telephone, FAX, a cellular phone, PHS, an electronic notebook, etc. which **********, or these combination. However, these components are not instantiation and all those components do not turn into an indispensable component of this invention.

[0017] The approach of concrete modification of a key is shown in drawing 5. For example, when there is Alice, an audience fee is paid, and it is assumed that it became a just addressee. A server assigns a key K7 to Alice, and enciphers and sends it with the public key of Alice. Moreover, the chain of what enciphered K3 by K7, K7 [i.e.,], (K3), and a series of keys which result in the session key of the root like K3 (K1) and K1 (K0) is further sent to Alice. When the number of the whole addressees is n, the magnitude of the key chain of Alice is like log (n). Here, the case where a carol leaves the set S of a viewer by a certain reason is considered. The carol has a key called K0, K1, K4, and K10 in her key chain. Therefore, in order not to make contents access a carol from now on, the recurrence line of these keys must be carried out, and the key of a carol must be made into an invalid (it is the key which attaches X of drawing 5).

[0018] Suppose that the recurrence line of K1 was carried out, and it considered as K1'. Then, since K1 which he has becomes an invalid, Alice needs to receive K3 (K1') which enciphered new K1' by K3. Similarly, it is necessary to tell an addressee about K0' by two key delivery packets called K1' (K0') and K2 (K0'). Thereby, Alice will know K1' and K0' and can see the contents enciphered by new session key K0' from a degree. Thus, since only the key relevant to the cryptographic key which a seceder has can be changed and the changed cryptographic key can be enciphered and distributed only to the addressee corresponding to the changed key with the key [directly under] of the key when a seceder comes out out of two or more addressees according to the hierarchical key structure of this invention, time and effort for renewal of a cryptographic key can be made into min.

[0019] Next, about the redistribution effectiveness of a key, it is as follows. For example, the number of packets required for the redistribution of a key when a carol secedes is calculated. since the key which the carol had is log2 (n) individual, the number of the keys which must be generated newly is also log2 (n) (if it says strictly -- the upper

method -- log2 (n) -- 1 -- small). It is necessary to encipher and send the key with the two children's key about one new key. Therefore, the number of key delivery packets required for the redistribution of a key is 2*log2 (n). If the case of an r-ary tree is generally considered, several p of a key redistribution packet will be set to p = r*logr(n) = r*log (n)/log (r). r to which n makes p min at the fixed time -- r=e -- it is (e is the bottom of a natural logarithm) -- since r is the natural number in fact -- the time of r= 3 is the optimal -- becoming -- the number of packets -- about 2.73* -- it is set to log (n). Again In the case of r= 2 If a binary tree is used, it will be actually more advantageous to use a quaternary tree in the case of r= 4, since the number of theory top packets is the same.
[0020] For example, it is assumed that n is broadcasting contents to 1 million, i.e., 1 million viewers. What is necessary is just to broadcast 2*log2 (106) individual, i.e., a 40 key redistribution packet, in the case of a binary tree, in order to remove one certain viewer. Since it is 2.73*log(106) =37.7 in the case of a ternary tree, if DES is used as a cipher system of a key, since one key can be sent by ID of a 64 bit + key, in ID of a key, the payload of a key delivery packet is 96 bits (12 bytes) also as 32 bits, and the whole is settled in 0.5 K bytes by this in 38 pieces.
[0021] Next, how to calculate two or more withdrawal collectively is shown below. When k persons secede collectively, it is not necessary to newly generate the key of a k*logr (n) individual. For example, it is because what is necessary is to update K0 only once. Moreover, when it turns out beforehand that several persons secede at a coincidence term, updating and the redistribution of a key when two or more withdrawal occurs can be made small by summarizing those viewers on the same possible branch (group) (when viewing and listening by the contract by the end of the month etc.). That is, an addressee's attribute performs a group division for two or more addressees beforehand, and if two or more addressees are matched with the key arranged hierarchical at the form of the tree structure according to the relation between groups, very efficient generation and distribution of a key can be performed. Moreover, contract years, a subscription stage, age, an occupation, the address, a firm, the telephone number, other individual information, etc. may be used as an addressee's attribute. It can change suitably irrespective of the essence of this invention.
[0022]
[Effect of the Invention] The distribution of an efficient cryptographic key it a specific viewer can be made to be able to participate dynamically or can be withdrawn is attained without being able to exhibit specification by this invention, in order to move on a known code technique, maintaining the interconnectivity of each company, and using an uphill circuit. Moreover, the whole security can be maintained however there may be a path with the problem on security in the middle of distribution.
[0023]